Department of Public Health and Human Services (DPHHS)

Health Insurance Portability and Accountability Act ("HIPAA") Privacy Policy

John Chappuis, Deputy Director

Date: November 19, 2002
Revised Date:

Policy Title:	Documentation and Record Retention		
Policy Number:	008	**Version:**	1.0
Approved By:			
Date Approved:			

Purpose:

This policy addresses the documentation and record retention requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

Policy:

General – DPHHS will maintain documentation required for HIPAA compliance and will store such documentation for a period of a minimum of six years and three months. Documentation that is no longer required will be destroyed in a manner appropriate to protection of the Protected Health Information ("PHI").

DPHHS will document all necessary policies for HIPAA compliance and will make all policies and procedures available to employees who deal with PHI in their work.

DPHHS will inventory all equipment, hardware and software, and will keep records of maintenance and security testing of such equipment.

DPHHS will document the offices or personnel who are responsible for receiving and processing authorizations to disclose PHI. All authorizations will be maintained on file for a period of six years and three months.

DPHHS will document the titles or offices responsible for receiving and processing access to PHI. Denial of access to PHI will also be documented by these offices or persons.

DPHHS will document the titles or offices responsible for processing requests to amend PHI. These offices will also document any circumstances where amendment was denied.

All DPHHS personnel who disclose PHI for purposes other than treatment, payment, health care operations, or in response to written authorizations will document such disclosures. The Privacy Officer will be responsible to collect and store such documentation logs for audit purposes. Patient requests for restrictions to uses and disclosures of PHI will be in writing and will be maintained by the Privacy Officer.

DPHHS will maintain documentation of training regarding privacy and security issues and will document which personnel have received such training and with what frequency.

DPHHS will maintain documentation of sanctions applied to employees for security violations.

The DPHHS Privacy Officer will document all circumstances where a patient has requested and received an accounting of disclosures of PHI.

DPHHS will maintain a file of Business Associate Agreements and contracts.

DPHHS will maintain records of all Notices of Privacy Practices and subsequent changes to those notices.

DPHHS will keep documentation of the classifications of personnel and their level of access to protected health information (See Information Security and Data Access Policy, December 15, 1996).

The Privacy Officer or office designated to receive complaints will maintain a file of complaints received and corrective actions taken.

Destruction of PHI

When documentation is no longer necessary or is otherwise scheduled for elimination, it will be destroyed in a manner to preserve protection of the PHI.

Paper documents will be shredded; and

Electronic records will be deleted and all back up storage will be erased or destroyed.

Procedure:

DPHHS will document all necessary policies for HIPAA compliance and will make all policies and procedures available to employees who deal with PHI in their work.
HIPPA policies and procedures will be kept in hard copy in binders at the nurse's stations on second and third floors and in the Health Information Area.
HIPPA policies and procedures will be available electronically from each computer in the facility.
Policies & procedures will be available electronically by clicking the policy & procedure icon.
Scroll through the index until you see HIPPA Policies, and then open the required policy. The policies are read only, but may be printed if necessary.

DPHHS will inventory all equipment, hardware and software, and will keep records of maintenance and security testing of such equipment.
Information Services Division, a division of DPHHS will complete this monitoring.

Each employee is assigned a CI number and chooses a password for each software program.
An inventory of all equipment, hardware and software is completed on a yearly basis.

DPHHS will document the offices or personnel who are responsible for receiving and processing authorizations to disclose PHI. All authorizations will be maintained on file for a period of six years and three months.
The Health Information Department will be responsible for receiving and processing all authorizations at MCDC. Employees have been trained to recognize an appropriate, completed and signed authorization form.
If there is a question regarding an authorization, the Supervisor will review the authorization prior to any action being taken on it. If the Supervisor is unavailable the facility Administrator will review the authorization for appropriateness. Along with HIPPA regulations, 45 C.F.R., Part 2 will be followed at all times.
If the release is approved the minimal necessary information will be sent to achieve the specified purpose of the disclosure.
A log of specific information sent, the party requesting the information, the patient name, date authorization signed, the first initial and last name of the person sending the information and the date the authorization received will be recorded electronically and sent to the State Privacy Officer on required dates.
Specific information sent, the date information sent, date authorization received and first initial and last name of person sending the information will be recorded on the authorization. The authorization will then be filed in the patient's medical record.

DPHHS will document the titles or offices responsible for receiving and processing access to PHI. These offices or persons will also document denial of access to PHI.
The Health Information Office will be responsible for receiving and processing PHI.
PHI may be copied, fax or mailed to the patient.
A charge for the cost of copying the record may be assessed to the patient.
If the patient is available on site, the record may be reviewed, with a professional staff person. The patient is not to review the record alone.
An electronic log of all information released or of patients reviewing their record will be maintained by the Health Information Department and will be transmitted to the State Privacy Officer as required.

DPHHS will document the titles or offices responsible for processing requests to amend PHI. These offices will also document any circumstances where amendment was denied.
The Health Information Department will keep an electronic log of all requests to amend PHI and the result of the request.

All DPHHS personnel who disclose PHI for purposes other than treatment, payment, health care operations, or in response to written authorizations will document such disclosures. The Privacy Official will be responsible to collect and store such documentation logs for audit purposes. Patient requests for restrictions to uses and disclosures of PHI will be in writing and will be maintained by the Privacy Official.

Information released without an appropriate authorization will be done only in the event of an emergency regarding the patient.
If information is released it will be documented in the patient medical record and maintained at the very front left hand side of the medical record. Information to be recorded is the name of the person giving the

information, date, specific information given, name-address-telephone of who the information was given to and the stated reason why the information was necessary.
The form to complete will be available in the health information area. If unable to locate a form, write the above information on a piece of paper.
Once the form has been completed and signed by the person transmitting the information give to the Privacy Liaison (Supervisor of Health Information) or put in appropriate mailbox.
Privacy Liaison will record the information in electronic format for transmission to the State Privacy Officer.
The original form or information will be filed in the patient's medical record by the privacy liaison. The State Privacy Officer may require and request a hard copy of this form.

DPHHS will maintain documentation of training regarding privacy and security issues and will document which personnel have received such training and with what frequency.
All staff at MCDC will be trained prior to April 13, 2003 and yearly thereafter.
All new employees will be trained during their orientation process.
The State Privacy officer will document in the employee record and in an electronic record for access training.
It will be the responsibility of the privacy liaison and/or the trainer to document the training.
The employee receiving the training will sign complete a HIPPA training test and sign the bottom of the test to show that training has been completed.
The privacy liaison will document the training in the electronic format for transmittal to the State Privacy Officer as required.
The personnel support staff will file the signed HIPPA training test in the employee's personnel file.

DPHHS will maintain documentation of sanctions applied to employees for security violations.
Electronic logs of all employees sanctioned and the results of such sanctions will be kept by the privacy liaison and transmitted electronically to the State Privacy Officer as necessary.
When an employee is found to have breached a patient's PHI/confidentiality depending on the circumstances of the breach and type of breach, necessary disciplinary action will be taken.
Steps of discipline may range from corrective counseling up to and including termination of employment, depending on the circumstances and severity of the breach of confidentiality.
All employees will have training regarding HIPPA regulations regarding Protected Health Information.
All employees will sign a Confidentiality Form stating that they will not share patient information without a appropriate, signed authorization form.

The DPHHS Privacy Officer will document all circumstances where a patient has requested and received an accounting of disclosures of PHI.
An electronic log will be kept to record all requests for an accounting of previous PHI information sent out.
Information on the log will be: patient name, date request received, date accounting sent, number of previous disclosures.
A hard copy of the accounting will be kept in the medical record at the front left hand side. This will be computer generated a signed by the Privacy Liaison.
The Privacy Liaison will keep the electronic log and transmit to the State Privacy Officer as required.

DPHHS will maintain a file of Business Associate Agreements and contracts
All Business Associate Agreements and contracts will be kept in central filing.

Business Associate Agreements will reflect HIPPA language.

DPHHS will maintain records of all Notices of Privacy Practices and subsequent changes to those notices. A Notice of Privacy Practices will be given to all patients upon admission. The Treatment Specialist helping with the admission will review and/or read the notice to the patient. The patient will then sign the last page of the form, the last page will be put in the Health Information box for filing in the patient's medical record and the patient will keep the remainder of the form for future reference.
As changes or updates of the form occur, a copy of each form prior to changes being made will be maintained in central filing.

DPHHS will keep documentation of the classifications of personnel and their level of access to protected health information (See Information Security and Data Access Policy, December 15, 1996)

The Privacy Official or office designated to receive complaints will maintain a file of complaints received and corrective actions taken.

Destruction of PHI

When documentation is no longer necessary or is otherwise scheduled for elimination, it will be destroyed in a manner to preserve protection of the PHI.

Paper documents will be shredded

Electronic records will be deleted and all back up storage will be erased or destroyed.

Procedure added 2/21/2003 MKH